بات‌نت ها: معماری و تکنیک های کشف آنها و چالش های پیش رو

امیر نبی زاده

علاقه‌مند و پژوهشگر آزاد در امنیت شبکه و برنامه نویسی

me@amirdaly.ir

چکیده : **بات‌نت‌ها نوع قابل توجهی از بدافزار هستند که عمده تهدیدات در حوزه امنیت اینترنت طی اقدامات و رفتارهای آنها در سطح شبکه و به صورت گسترده پراکنده شده اند. از آنجا که اینترنت بسیار سریع در حال رشد است، خطر بات‌نت ها نیز به سرعت در حال گسترش است. بسیاری از سازمان ها قربانیان حملات بات‌نت های هستند که منجر به کاهش و از دست دادن میزان قابل توجهی درآمد و سرویس آنها می شود. امروزه بات‌نت ها برای فرار و مخفی ماندن از سیستم های تشخیص، بسیار پیچیده تر و انعطاف پذیر تر شده اند. این مقاله برای درک و به روز رسانی اطلاعات، با هدف ارائه یک نمای کلی از بات‌نت است که شامل چرخه زندگی، تهدید و معماری می باشد. ما روش های تشخیص بات‌نت را طبقه بندی کرده و هر یک را با توجه به مکانیزم های خود از نظر نقاط قوت و ضعفشان مقایسه کرده ایم. همچنین در این مقاله در مورد چالش های موجود در حوزه ی بات‌نت که شامل اینده و روند تغییرات آنهاست نیز بحث خواهیم کرد.**

واژه های کلیدی: بات‌نت، چرخه حیات بات‌نت، چالش های بات‌نت، تشخیص بات‌نت، پروتکل های فرمان و کنترل.

۱- مقدمه:

بات‌نت به عنوان گروهی از تعداد زیادی از شبکه های کامپیوتری که کاری را به صورت اتوماتیک و یا وظیفه ای را به صورت از پیش تعیین شده برای یک مدیر بات یا نفوذگر انجام می دهد، گفته می شود. بات‌نت ها برای بسیاری از فعالیت های مخرب مانند ارسال هرزنامه، انجام حمله تکذیب سرویس توزیع شده[1] (DDoS)، انتشار بدافزارها و سرقت اطلاعات (داده های بانکی، حساب شماره و اطلاعات کارت اعتباری) استفاده می شوند. انجام این فعالیت ها نه تنها بر روی کاربران خانگی تاثیر می گذارد، بلکه موجب از دست دادن منابع مالی و اقتصادی سرویس دهنده اینترنت (ISP)، سازمان ها و دولت می شود.

در گذشته، بات‌نت های اولیه به عنوان ابزارهای مفید برنامه نویسان در ارتباط با سرور ها از راه دور محسوب می شد، اما در حال حاضر از آنها برای اجرای اعمال مخرب بر روی اینترنت استفاده می شود. هکرها بات‌نت ها را با استفاده از تکنیک های نفوذ به شبکه به وجود می آورند و از آنها به عنوان یک ابزار عمده جرایم اینترنتی که یک مشکل جدی برای امنیت اینترنت است، استفاده

[1] Distributed Denial Of Service

می کنند. اگر نرم افزار بات بر روی سیستم قربانی نصب شود آن را تبدیل به یک بات یا "زامبی[1]" می کند که یک هکر قادر خواهد بود از راه دور آن را کنترل نماید. بات‌نت می تواند یک گروه کوچک یا بزرگ بر اساس پیچیدگی برنامه های کاربردی آن باشد. علاوه بر این، قربانیان همیشه نمی دانند که از راه دور توسط مهاجمان کنترل می شوند.

به عنوان یک نتیجه از تحقیقات جالبی که در زمینه امنیت شبکه شکل گرفته است، بات‌نت ها یکی از خطرناک ترین تهدیدات سایبری محسوب می شوند. هرچند که بات‌نت های جدید هر روز در حال پیچیده تر و انعطاف پذیر تر شدن هستند تا در مقابل سیستم های تشخیص خود را در امان نگه دارند. در این مقاله ایده هایی برای کمک به محققان امنیتی در زمینه ی تهیه ی یک سیستم تشخیص بات‌نت کارامد و به روز، شرح و بررسی می گردد.

در این بررسی، ما ابتدا در بخش دو به مکانیزم بات‌نت ها خواهیم پرداخت که دیدی از خود بات‌نت و اجزای آن و چرخه ی حیات آنها فعالیت های مخرب آنها می دهد. سپس به معماری و انواع بات‌نت ها و دسته بندی های آنها خواهیم پرداخت. در بخش چهارم نیز راه های کشف بات‌نت را بررسی خواهیم کرد و مقایسه ای از لحاظ مزایا و معایب هر روش خواهیم داشت و در بخش انتهایی نیز چالش های حال و پیش روی حوزه ی بات‌نت را به بحث خواهیم گذاشت.

۲- مکانیزم بات‌نت

هدف از این بخش درک چگونگی عملکرد بات‌نت است. در این بخش به منظور بالا بردن اطلاعات پایه ای در زمینه بات‌نت و درک بهتر آن قبل از مباحث پیشرفته تر، به معرفی اجزای بات‌نت ، چرخه ی حیات و همچنین تهدیدات بات‌نت می پردازیم.

۲-۱- اجزای بات‌نت

بات‌نت شامل چهار جز اصلی است که شامل: مدیر بات[2]، اعضای بات‌نت[3]، پروتکل های کنترل و فرمان[4]، و سرور های کنترل و فرمان می باشد که در زیر شرح داده خواهد شد.

۲-۱-۱- مدیر بات

مدیر بات کسی است که کنترل و فرماندهی بات نت را برای انجام برخی از فعالیت های غیرقانونی (ارسال هرزنامه[5]، فیشینگ[6]، حملات توزیع شده ی تکذیب سرویس[7]، و ..) و همچنین مسئول حفظ بات‌نت از طریق ارسال به روز رسانی نرم افزارهای مخرب و انتشار بدافزار است.

۲-۱-۲- اعضای بات‌نت

[1] Zombie
[2] Bot master
[3] Bot clients
[4] Command and Control
[5] Spamming
[6] Phishing
[7] Distributed Denial of Service

بات یک کامپیوتر قربانی است که برنامه ی باتنت با مکانیسم های مختلف انتشار بدافزارها بر روی آن نصب شده است. گاهی اوقات یک بات است یک زامبی نامیده می شود. یک گروه از باتها و یا زامبی ها، اعضای باتنت نامیده می شوند. این اعضا دستوراتی که را که از سمت مدیر بات برای حمله به سرور هدف، به آنها ارسال می شود را دریافت می کنند.

۲-۱-۳- پروتکل های ارتباطی فرمان و کنترل[1]

پروتکل های ارتباطی فرمان و کنترل(C&C) [۱]، به پروتکل هایی گفته می شود که برای ارتباط بین مدیر بات و اعضای باتنت و یا بین بات ها استفاده می شود. اولین نسل از بات نت از رله چت اینترنت[2] (IRC) برای برقراری ارتباط استفاده می کردند. اعضای باتنت به سرور IRC متصل شده و منتظر دریافت فرمان از سوی مدیر بات می ماندند. با این حال، نقطه ضعف این ساز و کار یک نقطه از شکست است. برای مثال اگر سرور های IRC از دسترس خارج شوند و یا کشف شوند، کل اعضای باتنت به یک ارتش بی فایده تبدیل خواهند شد. برای حل اسن مشکل ، نسل دوم از باتنت ها به به پروتکل های نظیر به نظیر[3](P2P) روی آوردند. این مکانیزم مشکلات قبلی را ندارد اما از نظر مدیریت و کنترل بسیار دشوار است. بنابراین، مدیر بات به پروتکل HTTP برای ارتباط روی آورد. علاوه بر این، نسل جدیدی از باتنت ها نیز به وجود امدند که ترکیبی از پروتکل های نظیر به نظیر و HTTP هستند.

۲-۱-۴- سرور های فرمان و کنترل

این جز، سرور هماهنگ کننده بین مدیر بات و اعضای باتنت است. مدیر بات فرمان های خود را برای کنترل و یا به روز رسانی بات های خود، فرامین و یا فایل های به روز رسانی را از طریق این سرور ها ارسال می کند.

۲-۲- چرخه حیات باتنت

یادگیری چرخه حیات باتنت [۲] یک عامل مهم در تجزیه و تحلیل موفق از سیستم تشخیص باتنت است. درک هر مرحله از این چرخه می تواند به نوعی کمک به بهبود و توسعه یک سیستم تشخیص باتنت کارآمد باشد.

۲-۲-۱- آلوده کردن اولیه[4]

آلوده کردن اولیه مرحله اول است. در این فاز حمله کنندگان تلاش می کنند تا رایانه های قربانیان را با روش های مختلف نفوذ، آلوده کرده و اعضای جدیدی را فراهم نمایند. به عنوان مثال، ارسال ایمیل با فایل پیوست نرم افزارهای مخرب و یا یک

---
[1] C&C Protocols
[2] Internet Relay Chat (IRC)
[3] Peer to Peer
[4] Initial infection

لینک URL که منجر به نفوذ و آلوده شدن مرورگر می شود، و یا دانلود نرم افزار رایگان از اینترنت و یا سایت های مخربی که توسط حمله کنندگان ساخته شده است. حتی در مواردی هم مشاهده شده که نفوذگران به صورت مداوم در حال اسکن و نفوذ و آلوده سازی به صورت اتوماتیک در سطح اینترنت هستند.

۲-۲-۲- تزریق ثانویه[1]

مرحله ی دوم بلافاصله پس از پایان مرحله اول اجرا خواهد شد. اگر کاربر از همه جا بی خبر، پیوست های ایمیل ها را باز کند، کامپیوتر آلوده شده اش به صورت خودکار فایل هایی را از روی سرور شروع به دانلود می کند و زیرساخت بات بر روی ان سیستم کامل می شود. پس از پایان این مرحله، دستگاه یا کامپیوتر قربانی به یک بات یا زامبی واقعی تبدیل می شود. فایل های برنامه های بات معمولا از طریق پروتکل های HTTP، P2P و FTP دریافت می شود.

۲-۲-۳- جستجوی DNS[2]

اعضای جدید بات‌نت پس از تبدیل شدن به یک بات واقعی باید به سرور های فرمان و کنترل خود متصل شوند. اما همانطور که می دانیم فعالیت های بات‌نت ها غیر قانونی است. برای اختفا و فرار از سیستم های تشخیص و همچنین مدیریت بهتر، مدیر بات باید نام سرورهای فرمان و کنترل را ثبت کند. هر زمان که بات ها بخواهند با سرور فرمان و کنترل خود ارتباط برقرار کنند باید DNS آن سرور را جستجو و آدرس آن را پیدا کنند.

۲-۲-۴- اتصال[3]

گاهی اوقات به فاز اتصال، فاز گردآوری نیز می گویند. اگرچه دستگاه های قربانی با روش های مختلف تبدیل به بات می شوند، اما در نهایت بات های جدید باید به سرور فرمان و کنترل خود وصل شده و اعلام حضور کنند و یا اینکه اطلاعاتی در مورد سیستم های خود به سرور ارسال کنند. در این مرحله دستگاه زامبی به عضوی از اعضای ارتش بات‌نت تبدیل می گردد.

۲-۲-۵- دستورات مخرب[4]

پس از اتصال به سرور فرمان و کنترل، اعضای بات‌نت منتظر ارسال دستور از سوی مدیر بات می مانند. اگر انها دستورات را دریافت کنند، آنها را اجرا و فعالیت های مخرب را برای از پا دراوردن اهداف مورد نظر آغاز می کنند.

---

[1] Secondary injection
[2] DNS lookup
[3] Connection
[4] Malicious commands

۲-۲-۶- تعمیر و نگهداری و به روزرسانی[1]

آخرین مرحله از چرخه حیات بات‌نت تعمیر و نگهداری و به روزرسانی نرم افزارهای مخرب است. گام تعمیر و نگهداری یک مرحله مهم برای حفظ ارتش زامبی است. مدیر بات انگیزه های بسیاری از این اقدامات دارد. مثلا ممکن است مدیر بات بخواهد فایل های اجرایی بات خود را به روز رسانی و مشکلاتشان را رفع کند، و یا حتی آنها را هوشمندتر کرده و یا مکانیزم انها را برای جلوگیری از تشخیص ، تغییر دهد. به عنوان مثال می توان از تغییر رویه زمانی ثابت به متغیر جهت عملکردها و یا حتی تغییر آدرس سرور های کنترل و فرمان توسط این به روز رسانی ها نام برد.

۲- معماری بات‌نت ها

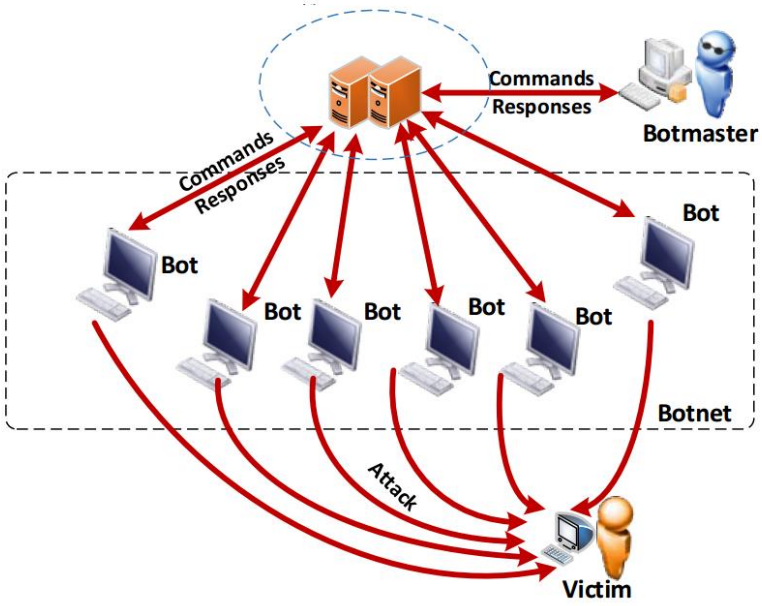
بات‌نت‌ها از کانالهای فرمان و کنترل[2] برای ارتباط با مدیر بات (دریافت فرامین و ارسال نتایج به وی) استفاده میکنند. بات‌نت‌ها را میتوان بر اساس کانالهای فرمان و کنترل به سه دسته تقسیم بندی نمود: مدل متمرکز ، مدل غیرمتمرکز و مدل ترکیبی[3] یا هیبریدی. در ادامه این بات‌نت‌ها مورد بررسی قرار میگیرند.

۲-۱- بات‌نت‌های متمرکز

مدل بات‌نت متمرکز همانند سرویس گیرنده/سرویس دهنده است. این مدل در ابتدا بر اساس IRC طراحی شد که در آن با استفاده از مکانیزم PUSH[۱۵]، ارتباطات برقرار می شد. ایده اینگونه بود که زامبی ها با اتصال به سرور IRC به یک کانال ملحق شوند و منتظر ارسال دستور از طرف مدیر بات بر روی این کانال باشند و به محض دریافت انها اقدامات دریافتی را انجام دهند.

شکل ۱ نمایی از بات‌نت با ساختار متمرکز مبتنی بر IRC را نمایش میدهد [۳].

[1] Maintenance and update
[2] Command and control (C&C)
[3] Hybrid Model



شکل ۱: نمایی از یک بات نت با ساختار متمرکز

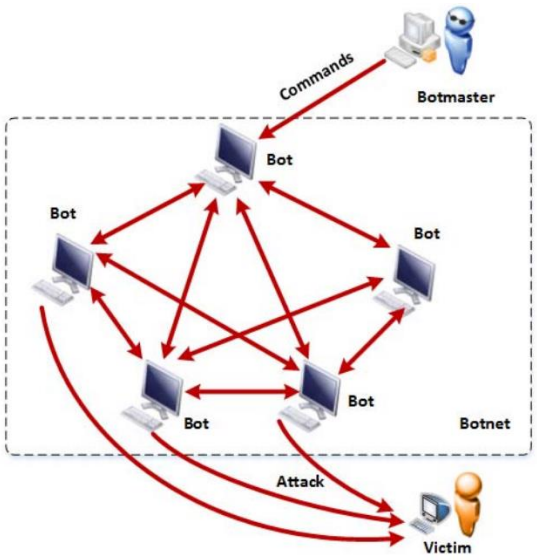
برای جلوگیری از تشخیص راحت و مخفی ماندن از سیستم های تشخیص نفوذ و فایروال ها ، باتنت ها از پروتکل های عمومی تری که تشخیص آنها از فعالیت های مخرب سخت تر و پیچیده تر است مانند HTTP استفاده کردند. چون با محدود و یا مسدود کردن پروتکل IRC در فایروال به راحتی از عملکرد باتنت ها جلوگیری میشد و یا قابل کشف بودند. در یک باتنت مبتنی بر HTTP، ابتدا مدیر بات یک سرویس‌دهنده وب برپا کرده و فرامین خود را در آن قرار میدهد. سپس بات‌ها به‌طور دوره‌ای از این سرویس‌دهنده سرکشی کرده تا جدیدترین فرامین را دریافت کنند. یکی از مزیت‌های این نوع بات مخفی ماندن ترافیک فرمان و کنترل در میان ترافیک HTTP معمول مرور[1] کاربران از صفحات وب است. اگرچه به راحتی میتوان باتنت‌هایی با ساختار متمرکز ایجاد نمود، اما این ساختار دارای یک ضعف عمده است. سرویس‌دهنده فرمان و کنترل نقطه یگانه شکست میباشد. از کار انداختن این سرویس‌دهنده باعث خواهد شد تا مدیر بات ارتباط خود با همه بات‌ها را از دست بدهد.

۲-۲- باتنت های غیر متمرکز

باتنت های غیر متمرکز را گاها "باتنت های توزیع شده" هم می نامند. در باتنت‌های غیرمتمرکز برای از بین بردن ضعف نقطه یگانه شکست، زیرساخت ارتباطی به طور کامل بر روی تنها یک و یا چند سرویس‌دهنده فرمان و کنترل استوار نیست. همچنین در این حالت با شناسایی تعدادی از میزبان‌های آلوده به بات، نمیتوان کل باتنت را از کار انداخت. در این باتنت‌ها، مدیر بات از یک پروتکل نظیر به نظیر برای برقراری ارتباط با بات‌های خود استفاده میکند. شکل ۲ نمایی از باتنت با ساختار غیرمتمرکز نظیر به نظیر را نمایش میدهد. در این نوع باتنت‌ها، هر بات به جای اتصال به یک سرویس‌دهنده فرمان و کنترل مرکزی به بات‌های همتای خود متصل شده و همزمان به‌عنوان متقاضی و سرویس‌دهنده عمل میکند. بنابراین اگر برخی از بات‌ها در یک باتنت تشخیص داده شوند، آن باتنت

[1] Browse

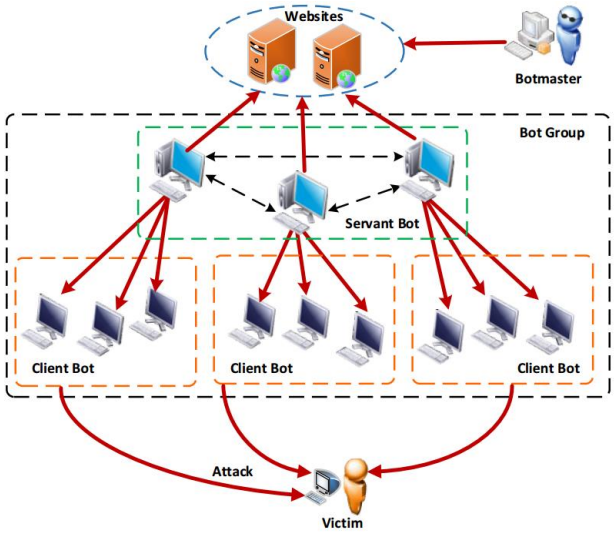
همچنان میتواند به فعالیتهای خود تحت هدایت مدیر بات ادامه دهد. مدیر بات فرامین خود را در اختیار یک یا چند بات برگزیده قرار داده و آنها این فرامین را در شبکه نظیر به نظیر پخش میکنند تا همه بات‌ها فرامین جاری وی را در اختیار داشته باشند.



شکل ۲:نمایی از یک بات‌نت با ساختار غیرمتمرکز

۲-۳- بات‌نت‌های ترکیبی

بات‌نت‌های ترکیبی هر دو ساختار متمرکز و توزیع‌شده را با یکدیگر ترکیب کرده و یا از یک ساختار تصادفی استفاده میکنند تا خودشان را در مقابل تشخیص مقاومتر سازند. برای درک بهتر این ساختار مثالی در شکل ۳ آورده شده است. با توجه به این شکل دو گروه از بات‌ها وجود دارند: خدمتگزار و کارگر. خدمتگذار بات‌هایی هستند که دارای آدرسهای IP ایستای عمومی بوده و به هر دو صورت متقاضی و سرویس‌دهنده عمل میکنند و همچنین از طریق اینترنت نیز در دسترس میباشند. آنها از اتصالات نظیر به نظیر استفاده کرده و فرامین مدیر بات را برای متقاضیان بازپخش میکنند. در سوی دیگر، متقاضیان بات‌هایی با آدرسهای IP پویای خصوصی بوده که در پشت دیواره‌های آتش و یا ادوات NAT قرار دارند که نمیتوانند اتصالات ورودی از اینترنت را بپذیرند. آنها همیشه به بات‌های خدمتگزار متصل شده تا فرامین جدید را به‌دست آورند.



شکل ۳ :نمایی از یک بات‌نت با ساختار ترکیبی

۳- چرخه حیات بات‌نت‌ها

بر خلاف سایر بدافزارها، بات‌نت‌ها چرخه حیات شفاف‌تری دارند که میتواند به سه مرحله اصلی شکل‌گیری، فرمان و کنترل، و حمله تقسیم شود. در هر مرحله نوع فعالیت بات‌نت‌ها متفاوت است. بهترین سیاست برای تشخیص آنها میتواند زمانی اتخاذ شود که مکانیزمهای هر مرحله به روشنی درک شود.

۴- تکنیک های کشف بات نت

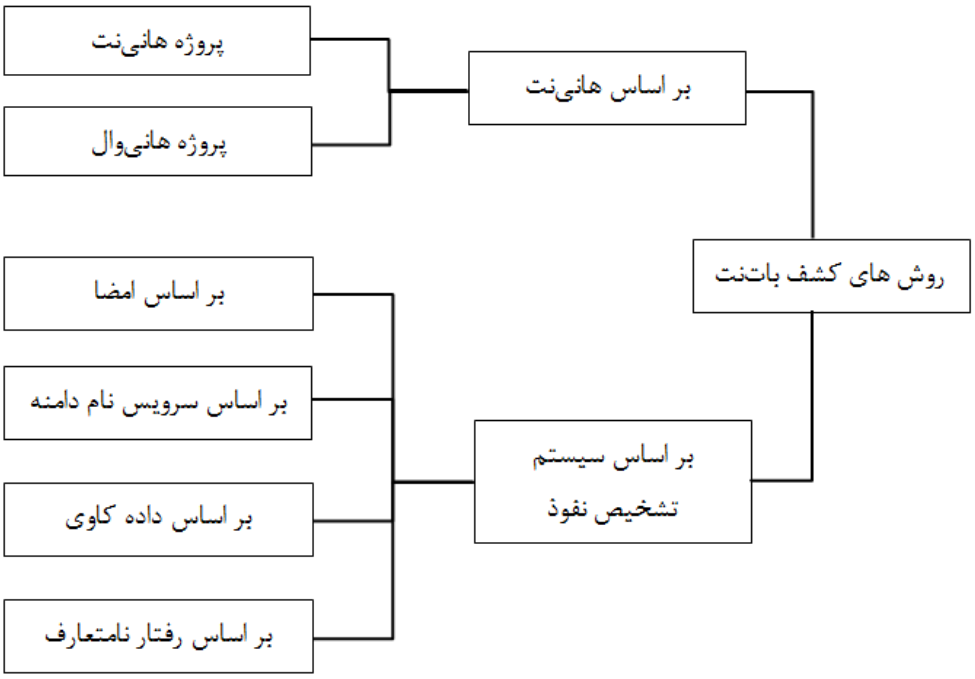
بات‌نت‌ها به عنوان مهمترین تهدید اینترنتی در سالهای اخیر شناخته شده‌اند. انواع جدید بات‌نت ها معمولا از تکنیک های فرار برای مخفی سازی خود از سیستم های کشف استفاده می کنند. این یک چالش بزرگ برای بسیاری از پژوهشگران حوزه امنیت محسوب می شود. به همین دلیل، تکنیک های کشف بات‌نت به یکی از موضوعات داغ پژوهش ها بدل شده است.

تکنیک های تشخیص بات‌نت به صور کلی به دو روش اصلی تقسیم می شوند. یکی از روش ها تکنیک مبتنی بر هانی‌نت[1] و دیگری روش مبتنی بر سیستم تشخیص نفوذ[2] می باشد.

پروژه ی هانی‌نت [۴] برای مطالعه ی رفتار بات‌نت ها در پژوهش های اخیر راه اندازی شد. این روش می تواند در شناخت فعالیت های بات‌نت، نتیجه‌گیری در مورد بات‌نت و همچنین مشخصه های بات نت به پژوهشگران کمک کند[۵]، اما نمی تواند بات‌نت را تشخیص داده و کشف کند. به علت محدودیت های پروژه ی هانی‌نت، تحقیقات و پژوهش های جدید در مورد کشف بات‌نت معمولا روش های

[1] Honey Net
[2] Intrusion Detection System (IDS)

مبتنی بر سیستم های تشخیص نفوذ (IDS[1]) که کاربردی تر هستند را استفاده می کنند. این روش های مبتنی بر سیستم های تشخیص نفوذ می توانند به چهار دسته تقسیم شوند: ۱- بر اساس امضا[2] ۲- بر اساس سرویس نام دامنه[3] ۳- بر اساس داده کاوی[4] ۴- بر اساس رفتار نامتعارف[5]



شکل ۴ : روش های کشف باتنت

۴-۱- بر اساس امضا

روش های بر اساس امضا ، بات نت ها را با مشاهده و زیر نظر داشتن جریان های شبکه و یافتن الگوهایی که با دانش گردآوری شده از باتنت های شناخته شده منطبق می گردد، کشف می کند[۶]. مزیت این روش ، یک تشخیص سریع و همچنین نیاز به منابع کمتر برای پردازش است. هرچند این روش با کشف باتنت های از قبل شناخته شده که در پایگاه داده ی امضاهای باتنت ها ثبت گردیده، محدود شده است.که این برای باتنت های ناشناخته و یا باتنت های جدید موثر نیست. بنابراین این روش اگر برای کشف باتنت های ناشناخته استفاده شود به طور کامل با شکست مواجه می شود. Snort [۷] یکی از IDS های شناخته شده ی متن باز است که از روش مبنی بر امضا برای مشاهده ی ترافیک شبکه و پیدا کردن امضاهای مشابه برای تشخیص نفوذ استفاده می کند.

[1] Intrusion Detection System
[2] Signature-based
[3] DNS-based
[4] Data mining-based
[5] Anomaly-based

Rieck [۸] در سال ۲۰۱۰ باتزیلا (BotZilla) را به عنوان یک روش مبتنی بر امضا به وجود آورد. روش مذکور باینری های بدافزارها را که از هانی‌نت های در حال کار هستند جمع آوری می کند. به عنوان مثال در یک نظارت بر بدافزار کشف شده ، واژه ی مرتبط با "تلفن به خانه" به عنوان امضا کشف شد که پس از آن مشاهده گردید که در تمامی باینری های بد افزارهای مشابه ، این فرمان نیز اجرا می گردد، بلافاصله به عنوان امضای اصلی این بات نت در نظر گفته شده و ضبط می گردد.

۴-۲- بر اساس رفتار نامتعارف

روش مبتنی بر رفتار نامتعارف به گونه ای است که با مشاهده و زیر نظر داشتن ترافیک شبکه ها و دسته بندی و آنها به عنوان ترافیک معمولی و متعارف کار می کند[۹]. این روش ممکن است موارد غیرمعمول ترافیک شبکه و فعالیت هایی نظیر حجم بالای ترافیک، ازدحام بالای شبکه، ترافیک بر روی پورت های غیرمعمول، و عملکرد غیرمعمول سیستم را نیز مشاهده کند. به طور کلی، روش مبتنی بر رفتار نامتعارف شامل دو مرحله می باشد. مرحله اول که به آن فاز یادگیری[۱] گفته می شود، این فاز یک الگوی متعارف از ترافیک[۲] شبکه خواهد ساخت. و مرحله ی دیگر فاز کشف رفتار نامتعارف خوانده می شود که در این فاز الگوی ساخته شده از ترافیک شبکه ی متعارف با ترافیک شبکه ی فعلی مقایسه می شود تا ترافیک نامتعارف را تشخیص دهد. سودمندی این روش این است که می تواند بات‌نت های جدیدی را که هنوز ناشناخته اند، و توسط روش مبتنی بر امضا قابل کشف نیستند را کشف کند. هرچند، این روش برای حملات جدید موثر است، اما نقطه ضعف این روش میزان بالای اشتباهات و سعی و خطای آن است.

GU و همکاران[۱۰]، یک فریمورک[۳] به نام BotMiner را معرفی کرد. روش معرفی شده فعالیت های ترافیکی بات نت را با زیرنظر داشتن الگوهای ترافیکی برای تفکیک بات‌نت از گروه های مشروع بر اساس رفتار و آمار ، کشف می کند. BotMiner ارتباطات مشابه و الگوهای رفتاری خطرناک را خوشه بندی کرده، و سپس یک ارتباط بین خوشه ای بین میزبان هایی که الگوهای مشابه دارند را برای تشخیص بات‌نت برقرار می کند.

۴-۳- براساس سرویس نام دامنه[۴]

روش مبتنی بر DNS شبیه روش مبتنی بر رفتار نامتعارف است با این تفاوت که این روش بر اساس اطلاعات DNS ای نامتعارف تولید شده توسط بات‌نت ها است. همانطور که در چرخه ی حیات بات‌نت اشاره شد، بات‌نت ها به سرور کنترل و فرمان خود برای گرفتن دستورات متصل می شوند. بنابراین، بات‌نت ها باید درخواست های DNS ی را برای یافتن یک سرور فرمان و کنترل مشخص ایجاد کنند که به طور مخصوص توسط یک سرویس دهنده DDNS[۵](سرویس نام دامنه ی پویا) ساخته شده است. از این مرحله ما میتوانیم با نظارت بر ترافیک DNS ، با تشخیص ترافیک نامتعارف DNS وجود بات‌نت را در شبکه تشخیص دهیم. این روش تنها در کشف بات‌نت موثر نیست، بلکه در پیدا کردن آدرس مدیر بات[۶] نیز کمک بسیاری را می کند. هرچندآنها ممکن است با استفاده از کمترین حد کوئری های DNS ، فرار کنند.

Choi و همکاران[۱۱]، یک روش بر اساس تحلیل ترافیک DNS در رفتار بات‌نت ها به نام BotGAD را پیشنهاد کردند. آنها یک مکانیزم سبک برای تشخیص بات‌نت ها با استفاده از فعالیت گروهی برای نظارت بر ردیابی درخواستهای DNS که از منابع

---

[1] Training phase
[2] Normal traffic profile
[3] Framework
[4] Domain Name Service (DNS)
[5] Dynamic DNS
[6] Botmaster

مختلف جمع اوری شده بود استفاده می کردند. آنها را بر این گرفتند که بات ها در یک دوره ی زمانی مشابه شروع به ارسال درخواست DNS می کنند و این یک الگوی رفتاری خاص است که بات نت ها استفاده می کنند و آنها را از گروه های مشروع و معمولی متمایز می کند.

۴-۴- بر اساس داده کاوی

از زمانی که بات‌نت ها تلاش بیشتری برای مخفی ماندن و فرار از سیستم های تشخیص انها هستند، گاهی اوقات تفکیک ترافیک معمولی و ترافیک نامتعارف بسیار سخت می شود. به عنوان مثال بات‌نت ها جدیدا از پروتکل های پرکاربرد برای ارتباط با سرور فرمان و کنترل خود استفاده می کنند که این تشخیص انها را به عنوان رفتار نامتعارف بسیار سخت می کند به علت اینکه رفتار کاملا معمولی ای از خود نشان میدهند. بنابراین ما به مزایای روش های متعدد مبتنی بر داده کاوی نیاز خواهیم داشت مانند یادگیری ماشین[1] که یکی از روش های موثر است به این علت که با درصد بالایی از موفقیت ترافیک های نامتعارف بات‌نت ها را از ترافیک معمول تفکیک می کند[۱۲].

جدول زیر روش های مختلف تشخیص بات‌نت را با هم مقایسه می کند.

روش کشف	بات‌نت ناشناخته	مستقل از پروتکل	کشف رمزنگاری شده	کشف آنی	درصد خطای کم
مبتنی بر امضا	خیر	خیر	خیر	خیر	بلی
مبتنی بر DNS	بلی	خیر	بلی	خیر	بلی
مبتنی بر رفتار نامتعارف	بلی	بلی	بلی	خیر	خیر
مبتنی بر داده کاوی	خیر	بلی	بلی	خیر	بلی

جدول ۱: مقایسه ی روش های کشف بات‌نت

۵- چالش های حوزه ی بات‌نت

۵-۱- کشف بات‌نت در مقیاس کوچک[2]

بسیاری از روش های کشف بات‌نت ، ترافیک های بات‌نت هایی را آنالیز می کنند که توسط بات هایی در بات نت های یکسان تولید شده اند. این روش ها مستلزم وجود تعداد زیادی بات در یک بات‌نت است تا بتوان تصمیم درستی اتخاذ کرد. از این رو ، آنها تاثیرگذاری کمتری در بات‌نت های در مقیاس کوچکتر و یا یک بات به تنهایی هستند.

۵-۲- نرخ بالای هشدار اشتباه[3]

کنترل کننده های بات از مزایای سرویس های HTTP برای پنهان کردن فعالیت های خود از فایروال ها و سیستم های تشخیص نفوذ استفاده می کنند، و این به علت وسعت و تنوع HTTP سرویس های کاربردی به سادگی قابل مسدود نیست. الگوهای ترافیکی ای که بات‌نت های HTTP ایجاد می کنند بسیار به الگوهای ترافیکی سرویس های HTTP معمولی شبیه است. از این رو

[1] Machine learning (ML)
[2] Small-Scale
[3] High rate of false alarm

، تحلیل و تشخیص این باتنت ها با کمترین میزان خطا بسیار سخت است و به یک چالش جالب در حوزه باتنت ها مبدل شده است.

۵-۳- تغییر روش باتنت ها

بسیاری از فریمورک های تشخیص و کشف، از محدوده ی اثرگذاری کوتاهی بهره می برند چرا که حمله کننده ها به صورت مداوم در حال تغییر روش ها و استراتژی های خود در جهت پنهان ماندن از این سیستم ها هستند و هر روزه باتنت ها انعطاف‌پذیر تر می شوند که این باعث می گردد تشخیص انها بسیار سخت شود. برای مثال آنها قسمتی یا حتی کل باینری های بدافزارهایشان را تغییر داده و یا حتی روش های فعالیت خود را از حالت عادی به حالت تصادفی تغییر میدهند. هرچه میگذرد آنها نیز فناوری های جدید را در سیستم های خود دخیل می کنند مانند سرویس های ابری و موبایل. از این رو این مشکل نیز به چالشی جدید در حوزه ی محققان امنیتی تبدیل شده است.

۵-۴- جلوگیری و کاهش آلودگی

بسیاری از مطالعات در حوزه باتنت به نحوه ی کشف آنها می پردازند. مطالعات جدی ای هم در حوزه ی جلوگیری و کاهش آلوده شدن سیستم ها توسط باتنت ها وجود دارد. بیشتر مطالعات در حوزه ی جلوگیری از آلودگی به باتنت به بخش کشف باتنت ها در موقعیت زمانی زودتر می پردازد. از طرف دیگر، مطالعات بیشتری نیز در حوزه ی کاهش آلودگی و همچنین عکس العمل در برابر آلودگی سیستم ها انجام می شود. از این رو ، جلوگیری و کاهش آلودگی به باتنت نیز چالش های جذابی هستند.

۵-۵- کشف آنی

روش های کشف باتنت معمولا لاگ شبکه را برای پیدا کردن ردپای حضور باتنت ها آنالیز میکنند، مخصوصا روش های مبتنی بر رفتار نامتعارف که لاگ های گوناگون ترافیک را برای یافتن ارتباط رفتار های غیرمعمول ، بررسی و تحلیل می کند. به همین دلیل، کشف و تشخیص آنی و در لحظه ی یک باتنت، یکی از چالش های باتنت در نحوه ی پردازش و تحلیل حجم عظیمی از لاگ ها و ترافیک های شبکه است که این کار را در لحظه و به صورت آنی بسیار سخت کرده است.

۵-۶- بات ابری[1]

میزبانی سرویس های شبکه بر روی پلتفرمهای ابری[2] روز به روز گسترده تر می شود. باتمستر از ویژگی ها و مزایای پلتفرمهای ابری برای آلوده‌کردن سرویس های ابری به جای کاربران انتهایی استفاده می کند و ما به این نوع از باتنت ها "BotCloud"[۱۳] یا بات ابری می گوییم. منافع زیادی در اجرای بات ابری وجود دارد که به عنوان مثال می توان راحتی در ساخت، آنلاین بودن دایمی، قدرت پردازشی بالا، هزینه ی کم و امنیت کمتر اشاره کرد. در حال حاضر امنیت سرویس های ابری بسیار پایین می باشند و آلودگی و تکثیر و پنهان ماندن باتنت در آنها به باتمستر این امکان را می دهد تا به راحتی به فعالیت های خود ادامه دهند.

۵-۷- باتنت های موبایل

[1] BotCloud
[2] Cloud Platforms (CP)

با ازدیاد و همه گیر شدن استفاده از تلفن های هوشمند ، بات‌مستر ها را برای مهاجرت دادن بات‌نت ها به روی دستگاه های موبایلی ترغیب کرده است. تلفن های هوشمند دستگاه هایی فوق العاده برای جولان بدافزار ها شده اند زیرا از زیرساخت ها و فناوری های متعدد و گوناگونی در خود بهره می برند. فناوری هایی اعم از 3G,4G,WiFi, SMS, MMS, Bluetooth [۱۴] . بنابراین آنها می توانند راه ها و فناوری های متعددی را برای تکثیر و اجرای بات‌نت ها به کار گیرند. به دلیل پیچیدگی و انفرادی بودن دستگاه های تلفن هوشمند، امن سازی آنها به طبع سخت تر از امن سازی یک شبکه ی محلی با مدیریت متمرکز خواهد بود و به همین دلیل این دستگاه های هوشمند بسیار مورد علاقه ی بات‌مستر ها قرار گرفته اند.

۶- نتیجه‌گیری

در این مقاله هدف ما بررسی وضعیت فعلی بات‌نت ها و اینکه چگونه کار می کنند و همچنین دادن ایده هایی برای سیستم های تشخیص و کشف آنها بود. همانطور که در جدول ۱ مشاهده کردیم ، روش تشخیص بر مبنای رفتار غیر متعارف برای بات‌نت های ناشناخته و جدید بسیار موثرتر از روش های است اما در عین حال میزان خطای بسیار زیادی نیز دارد. در مقابل رویکرد مبتنی بر داده کاوی دقت بالایی را فراهم می سازد در حالی که تاثیر این روش در تشخیص بات‌نت های جدید و ناشناخته بسیار ناچیز است. بنابراین ترکیبی از این دو تکنیک ، می تواند نقاط ضعف یکدیگر را پوشش داده و عملکردشان را بالا ببرد. علاوه بر این یک عامل مهم و اساسی برای شناسایی و تشخیص، ترافیک شبکه است، اما رشد روز افزون ترافیک و گسترش حجم اینترنت به عنوان یک مشکل بزرگ بر سر راه قرار دارد چرا که پردازش آنی این حجم عظیم از اطلاعات بسیار زمانگیر و هزینه بر خواهد بود. به منظور رسیدگی به این چالش ما استفاده از مزایای سیستم های منبع باز مانند Hadoop و MapReduce را که برای بهینه سازی عملکردشان از مدل های محاسبات توزیع شده استفاده می کنند را پیشنهاد می کنیم. و پس از آن از لحاظ تکنیکی ترکیبی از دو روش مبتنی بر داده کاوی و مبتنی بر رفتار نامتعارف را مفید و موثرتر خواهیم دید.

مراجع

[1] R. A. RODR´IGUEZ-GO´ MEZ, G. MACIA´- FERNA´NDEZ, P. GARC´IA-TEODORO, “Survey and Taxonomy of Botnet Research through Life-Cycle,” ACM Computing Surveys, Vol. 45, Aug 2013.

[2] S. S.C. Silva, R. M.P. Silva, R. C.G. Pinto, “Botnets: A survey,” Computer Networks, Vol 57, pp 378-403, Febuary 2013.

[3] J. Oikerinenand D. Reed,“Internet Relay Chat protocol”, Web Publication, http://tools.ietf.org/html/rfc1459#section1, 2006.

[4] P. Bacher, T. Holz, M. Kotter, and G. Wicherski, “Know your enemy: Tracking botnets,” http://www.honeynet.org/papers/bots/, 2005.

[5] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” in Proc. 6th ACM.

[6] M. Feily, A. Shahrestani, S. Ramadass, “A Survey of Botnet and Botnet Detection,” IEEE International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), pp. 268-273, June 2009.

[7] Snort IDS web page. http://www.snort.org, March 2006.

[8] K. Rieck, G. Schwenk, T. Limmer, T. Holz, P. Laskov, “Botzilla: detecting the ’’phoning home’’ of malicious software,” Proceedings of the 2010 ACM Symposium on Applied Computing, pp. 1978–1984, March 2010

[9] C. Chen, H. Lin, “Detecting botnet by anomalous traffic,” Journal of Information Security and Applications, pp. 1-10, July 2014.

[10] G. Gu, R. Perdisci, J. Zhang, and W. Lee, “Botminer: clustering analysis of network traffic for protocol and structure-independent botnet detection,” in USENIX Security Symposium (SS), San Jose, CA, pp. 139–154, July 2008.

[11] H. Choi, H. Lee, “Identifying botnets by capturing group activities in DNS traffic,” in ScienceDirect, Computer Networks, Vol 56, pp.20–33, January 2012

[12] Stevanovic, Matija, Pedersen, J. Myrup, “Machine learning for identifying botnet network traffic,” Aalborg University, 2013

[13] P. Hayati, “botCloud – an emerging platform for cyberattacks,” the Cloud Security Research Group of the Stratsec Winter School, Sunday, October 2012.

[14] M. Eslahi, R. Salleh, N. Badrul Anuar, "MoBots: A New Generation of Botnets on Mobile," International Symposium on Computer Applications and Industrial Electronics (ISCAIE 2012),pp. 262-266 December 2012.

[15] M. Eslahi, “HTTP-Botnets: The Dark Side of a Standard Protocol!,” Cyber Defense Magazine, pp 12-18, April 2013.